
# IT Service Management (ITSM) Configuration Management Policy

Table of Contents



# Purpose

The purpose of this Policy is to establish a DMDC wide Configuration Management Program and to provide responsibilities, compliance requirements, and overall principles for Configuration Management process that supports information systems and technology management across all of the DMDC.

# Scope

## In scope:

This DMDC Configuration Management policy applies to employees, contractors, consultants, and other workers at the DMDC, including all personnel affiliated with third parties who have a need to implement a change to any DMDC configuration item (CI). This includes but is not limited to modifications to any configuration item in the following environments:

- Production (including 24x7)
- Contractor Test (CT)
  - Demo1 and Demo2
- Disaster Recovery (DR)
- Stress Test
- QA
  - Model1 and Model2
- DEV
  - Test1 and Test2

### Out of scope:

The following areas are out of scope for this policy unless explicitly identified and shall be governed by the applicable policies for each:

- Development and lab environments not specifically referenced as being "In Scope" of this policy.
- Mainframe Platforms at the NPS (Naval Post graduate School)
- Service Request and Incident related activities for individual workstations, laptops, printers and other DMDC standard devices at the unit level (outside the scope of DMDC domain or Organizational Unit (OU) policy, patching requirements, etc.)
    - For example: Individual workstations and laptops used for general business purposes; workstations used for code generation, code testing or other individual purposes.

## Policy Statements

| Policy No. | Change Management Policy |
|---|---|
| **CfgM-x** | DMDC shall establish, implement, and enforce configuration management controls on all services, systems, networks and applications deemed to be in-scope of this policy. |
| **CfgM-x** | The Information Assurance requirements will be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DMDC information systems configurations. |
| **CfgM-x** | Every change or modification to a DMDC managed configuration is subject to the Change Management Policy and must follow the approved DMDC Change Management process and related procedures. |
| **CfgM-x** | Configuration Management shall be performed by documenting requirements; maintaining consistency between critical assets and their respective critical administrative information and approved configurations; and ensuring that approved changes to configurations are reflected in the configuration documentation. |
| **CfgM-** | There shall be a documented procedure for recording, controlling and tracking versions of CIs. The degree of control shall maintain the integrity of services and service components taking into consideration the service requirements and the risks associated with the CIs.<br>• All changes to work products under configuration management control, i.e. Configuration Items (CI), will be tracked and controlled by means of a change request.<br>• Configuration items will be identified in the change or release request form and |

| Policy No. | Change Management Policy |
|---|---|
| | before any change is implemented to the configuration item.<br>• Records of configuration items will be established and maintained as defined in the CM plan. |
| **CfgM-x** | Configuration Management Database (CMDB):<br>• The organization will use a single or federated repository for storing all information related to hardware and software configuration items and the associated configuration management relationships / dependencies.<br>• Changes to CIs shall be traceable and auditable to ensure integrity of the CIs and the data in the CMDB.<br>• Master copies of CIs recorded in the CMDB shall be stored in secure physical or electronic libraries referenced by the configuration records. This shall include at least documentation, license information, software and, where available, images of the hardware configuration. |
| **CfgM-x** | Configuration Management process will implement and ensure that a regimented set of standard operating procedures (SOPs) are followed, to include but not limited to:<br>• Configuration Identification: Selecting and identifying the configuration structures for the entire infrastructure CIs, including the owner, interrelationships, and configuration documentation.<br>• CI Naming Conventions, Classification and Relationships: CIs shall be uniquely identified and recorded in a CMDB. The CMDB shall be managed to ensure its reliability<br>• and accuracy, including control of update access.<br>• Configuration Control: Ensuring that only authorized and identifiable CIs are accepted and recorded from receipt to disposal.<br>• Configuration Status Accounting: The reporting of all current and historical data concerned with each CI throughout its life cycle.<br>• Configuration Verification and Audit: A series of reviews and audits that verify the physical existence of CIs and check that they are correctly recorded in the CMDB. |
| **CfgM-x** | Configuration Baseline:<br>• A configuration baseline of the affected CIs shall be taken before deployment of a release into the live environment. |

| Policy No. | Change Management Policy |
|---|---|
| | • Configuration of critical DMDC assets shall be documented in configuration management tool at levels necessary to design, construct, operate, support and dispose of an asset.<br>• The level of detail documented shall be tailored and proportionate to the product's scope, importance, complexity, production quantity, performance requirements, budget, and schedule.<br>• At a minimum, the configuration baseline shall identify the product's performance, functional, and physical attributes, including internal and external interfaces.<br>• The baseline shall also include traceability of the lowest level configuration items (CIs) to the highest level requirements (i.e., a traceability matrix).<br>• Authorized deviations from an asset's configuration baseline shall be documented. |
| | Asset Management<br>• There shall be a defined interface between the configuration management process and the asset management process.<br>• All assets used to deliver services will be managed according to relevant statutory, regulatory and financial requirements and contractual obligations. Assets will be managed by effective procedures.<br>• Asset management requires an accurate configuration management database (CMDB), or equivalent means of record keeping, to be established and used effectively. Information in the CMDB will be kept current by effective service management processes, e.g. changes to the CMDB to be approved via the change management process. |
| **CfgM-x** | Documentation<br>• All designated documentation relating to the processes of configuration management and deployment will be placed under configuration and change management control.<br>• Note: Designated work products include, but are not limited to, roles and responsibilities, standards, guidelines, process descriptions, procedures, templates, SOPs and work instructions. |
| **CfgM-x** | Stakeholders:<br>• Stakeholders in the relevant configuration management and deployment processes |

| Policy No. | Change Management Policy |
|---|---|
| | will be identified and engaged as necessary.<br>• A list of relevant stakeholders will be established and maintained. |
| **CfgM-x** | Configuration Audit:<br>• The final step in any approved change will be an update and verification of the CMDB. The Configuration Manager will oversee the verification of CIs in the change record.<br>• The service provider shall audit the records stored in the CMDB, at planned intervals. Where deficiencies are found, the service provider shall take necessary actions and report on the actions taken.<br>• Configuration audits shall be performed to verify that configuration management requirements have been met and that the requirements have been accurately documented before a configuration is baselined or is migrated to the production environment. In addition, developmental and operational systems shall be periodically reconciled against their documentation to ensure consistency between production and its current baseline documentation. Verification of the incorporation of modifications is a critical function of this activity. Periodic audits of software and hardware configuration baselines in the production environment shall be performed to ascertain that no unauthorized changes have been made without proper approval. |
| **CfgM-x** | Management Oversight:<br>• The status of the configuration management process and practices will be reviewed with senior management on a regular basis<br>• Issues identified will be logged and resolved as part of the Continual Service Improvement program. |

## Roles and Responsibilities

This policy calls for specific roles to be filled to ensure the effectiveness and efficiency of the Configuration Management process. The names of the DMDC personnel who will fill these roles will be documented and updated in the Configuration Management Process documentation and associated RACI matrix.

| Role | Responsibility |
|---|---|
| Process Owner | The Process Owner is accountable for the effectiveness of the process and efficiency of the supporting documentation for the process. This includes |

| Role | Responsibility |
|---|---|
| | accountability for setting policies and providing leadership and direction for the development, design and integration of the process as it applies to other applicable frameworks and related ITSM processes being used and / or adopted for the DMDC. The Process Owner will be accountable for the overall health and success of the Configuration Management Process. |
| Process Manager | A role officially assigned to a single individual who will be accountable for all activities associated with the DMDC Configuration Management process. The Configuration Management process manager manages execution of the Configuration Management process and coordinates all activities required to process and manages changes. The Configuration Management process manager has the ultimate responsibility for the use of the Configuration Management process and procedures. |
| DMDC Leadership | It is the responsibility of all managers and leaders within the DMDC to ensure that all personnel subject to this policy are aware of this policy and are adequately trained to adhere to it. |
| DMDC employees and contractors | It is the responsibility those DMDC employees and contractors who participate in the Configuration Management process to read, understand and work within the guidelines set forth in this policy and the related processes and procedures. |

## Exceptions

- Requests for exception to this policy must be submitted in writing to the Process Owner.
- Request exception will be reviewed by the Process Owner and must be further reviewed and approved by the DMDC Change Advisory Board (CAB).

## Enforcement

Any violations of this policy shall be reported to the appropriate member of management.

In the event that the DMDC Management believes a violation of this policy has occurred and the conduct is capable of being addressed, it shall notify the employee and/or supplier and provide a reasonable opportunity to address such circumstances as it believes constitute a violation of this policy.

## Policy Approval

| Approvers | Title and/or Affiliation | Approval Date |
|---|---|---|
| Kris Hoffman | Chief Information Officer, DMDC and Process Champion | |
| Wade Shaffer | Director, Systems and Technical Support Division, DMDC | |

## Version Control

This DMDC Configuration Management Policy supersedes all existing Configuration Management policies or references to management of configurations made in previously published DMDC Change Management, TRB-CCB or Configuration Management documentation.

| Version | Date | Author | Change Description |
|---|---|---|---|
| 1.0 | 27 April 2014 | Corde Wagner | Initial Rewrite – Draft |

## References


- DMDC Change Management TRB/CCB Procedure Document, v17, August 2013
- Management of the Department of Defense Information Enterprise, DoD Directive 8500.01 and 8500.02
- Recommended Security Controls for Federal Information Systems and Organizations, NIST 800-53 rev-4, National Institute of Standards and Technology, US Department of Commerce, 4/30/2013
- ISO/IEC 20000-1:2011, Clause 9.1
- COBIT v5 Enabling Processes, ISACA, 2012
- ITIL Service Strategy, v3, TSO, 2011
- ITIL Service Design, v3, TSO, 2011
- ITIL Service Transition, v3, TSO, 2011
- ITIL Service Operation, v3, TSO, 2011